TRANSLATION

of DE 195 21 902 A1 (SEL ALCATEL AG)
Col. 1, line 64 to Col. 5, line 50

...

In the following the invention is explained by way of two embodiments and with the aid of Figs. 1 to 5:

Fig. 1 shows a schematic representation of a first embodiment of the inventive security system for motor vehicles,

Fig. 2 shows a schematic diagram of an inventive security device for the security system of Fig. 1,

Fig. 3 is a schematic representation of a control unit for the inventive security device of Fig. 2,

Fig. 4 is a schematic diagram of an inventive control centre for the security system of Fig. 1, and

Fig. 5 is a schematic representation of a second embodiment of the inventive security system for motor vehicles.

A first embodiment of the invention is now described in accordance with Figs. 1 to 4.

Fig. 1 shows a first embodiment of an inventive security system SYS comprising a radio system FS, a motor vehicle KFZ and an ignition key ZS. The security system SYS serves for protecting motor vehicles KFZ against unallowed use from a control centre ZE via radio signals. For the sake of explaining the invention, only the securing of one motor vehicle in one radio cell of the radio system FS is described. The same applies to securing several motor vehicles in several radio cells.

The motor vehicle KFZ, e.g. passenger car or motor lorry, contains a security system SE with an antenna through which the security system SE can communicate with the control centre ZE. The antenna is for example an antenna of a GSM-mobile station, which may be contained in the security device.

The radio system FS is configured as a cellular mobile radio system according to GSM-standard; GSM stands for Global System for Mobile Communication. Such a cellular mobile radio system is for example known

from the book "The GSM System for Mobile Communications", 1992, M.Mouly and M. Pautet, Int. Standard Book Number 2-9507190-0-7, pages 94 to 98 and 309 to 312. The radio system FS comprises a fixed radio station BTS, a fixed radio station control BSC, a radio exchange MSC and the control centre ZE. The fixed radio station BTS is connected to the control centre ZE via the fixed radio station control BSC and the radio exchange MSC.

The ignition key ZS contains an infrared-transmitting unit IRS, a counting device N and a switch S operable by touch of the finger. The infrared-transmitting unit IRS serves for transmitting infrared signals to the security device SE in the motor vehicle KFZ. The counting device N is a device for generating binary bit sequences of fixed length, wich are transmitted to the security device SE via the infrared-transmitting unit IRS and the value of which changes with each transmission. The counting device N is controlled via switch S. The count of the counting device N is increased by each actuation of the switch S by one unit and transmitted via the infrared-transmitting unit IRS.

Fig. 2 shows a schematic diagram of the security device SE of Fig. 1.

The security device SE comprises three means AN, ZD, KP which are required for starting the motor vehicle KFZ, i.e. a starter AN, an ignition coil ZD and a fuel pump KP, each with electronic control. The security device SE serves for making the three means AN, ZD, KP electronically ready for operation or to block them. For this purpose the security device SE contains a control device CTRL, an infrared-receiving unit IRE, a transmitting equipment SEN, a receiving equipment EMP and an antenna ANT. The control devic CTRL controls the three means AN, ZD, KP in response to the signals received via the infrared-receiving unit IRE and the receiving equipment EMP. For this purpose, the control device CTRL is connected with the three means AN, ZD KP, the infrared-receiving unit IRE, the transmitting equipment SEN and the receiving equipment EMP. The transmitting equipment SEN and the receiving equipment EMP are connected with the antenna ANT.

Fig. 3 shows a schematic representation of the control device CTRL of Fig. 2.

The control device CTRL comprises a computing unit RE, e.g. a microprocessor having two inputs and three outputs. The first output is connected with the ignition coil ZD, the second output with the starter AN and the third output with the fuel pump KP. The ignition coil ZD, the starter AN and the fuel pump KP are made ready for operation in response to the signals applied to the two inputs of the computing unit RE, whereby for example the voltage supply for the ignition coil ZD, the starter AN and the fuel pump KP, each, is connected via a relais. Each time the engine is switched off, ignition coil ZD, starter AN and fuel pump KP are blocked by the computing unit RE in that, for example, the voltage supply via a relais is cut off. For this purpose, for example, a control signal is transmitted from the engine control to the computing unit RE as soon as the engine is switched off. A renewed startup of the motor vehicle KFZ is only possible via new input signals for the computing unit RE. The new input signals have to differ from the input signals of the previous startup. A first input signal for the control device CTRL is derived from the infrared-signal of the igntion key ZS, a second input signal from the radio signal of the control centre ZE. If both input signals are identic, ignition coil ZD, starter AN and fuel pump KP are made ready for operation.

The control device CTRL further incorporates a comparator VER, an updating unit AKT, a memory MEMO, a read-in unit IN, a read-out unit OUT and an identification unit ID. First, the infrared signal of the ignition key ZS is supplied to the comparator VER. Inside the comparator VER a comparison between the count, contained in the infrared signal and a count stored in the updating unit AKT takes place. If the count of the infrared signals is at least by one unit and at most by ten units higher than the count of the updating unit AKT, the infrared signal is transferred and the count in the updating unit AKT is replaced by the count of the infrared signal. Having passed the comparator VER the infrared signal is supplied to the identification unit ID. Inside the identification unit ID an individual indentification number of the

motor vehicle KFZ is added to the count of the infrared signal. Both, count and identification number on the one hand serve as a first input signal for the computing unit RE and on the other hand form a request signal which is radio-transmitted via the transmitting equipment SEN of the security device SE to the centre ZE.

The centre ZE evaluates the request signal, checks if the identification number is contained in a database, and - if the identification number is in the database - transmits five encoded radio signals to the control device. The five encoded radio signals are read-in into the memory MEMO via a read-in unit IN and are stored. The first encoded radio signal contains the count of the infrared signal and the identification number in encoded form and is stored under the memory address corresponding to the count of the infrared signal. The second encoded radio signal contains the count increased by one unit and the identification number and is stored under the memory address with the value of the count increased by one unit. The same applies to the third, fourth and fifth radio signals.

The control device CTRL further contains an exclusive-OR-gate XOR, an RSA decoding unit RSA and a read-only memory KEY2, wherein a public key is stored. RSA means Rivest, Shamir, Adleman. According to RSA signals can be asymmetrically encoded and decoded. The encoding method according to RSA is for example known from the book "Chipkarten-Technologie in der Anwendung"*, 1995, pages 47 to 54, Wissenschaftsverlag Volker Spiess GmbH, Berlin, ISBN 3-89166-183-5. *[Chip card technology and application thereof].

The centre ZE encodes signals by a secret key according to the RSA-algorithm. The secret key, for example, is 512 bits long and only known to the centre ZE. For decoding in accordance with the RSA-algorithm, the control device CTRL in the motor vehicle KFZ incorporates a public key, which may be used for several motor vehicles KFZ and which may also be known to the public.

The exclusive-OR-gate XOR has two inputs and one output. The output is connected via the RSA-decoding unit RSA with the second input of the

computing unit. The count of the infrared signal is applied to the first input. The memory contents belonging to the memory address corresponding to the count of the infrared signal are applied to the second input. Thus, the contents of the memory are linked with the count of the infrared signal, supplied to the RSA-decoding unit RSA and decoded, and supplied to the computing unit RE to be compared with the identification number and the count of the infrared signal. In case of agreement the ignition coil ZD, the starter AN and the fuel pump KP are made ready for operation so that the motor vehicle KFZ may be started.

Thus, five encoded radio signals are on stock in the memory MEMO, by means of which the motor vehicle KFZ may be started five times without having to receive radio signals from the centre ZE in advance. This, for example, is necessary for starting the motor vehicle KFZ at places like underground parkings, where no radio signals can be received. After five starts of the motor vehicle KFZ and without any further radio signals from the centre ZE, another start of the vehicle is impossible. Hence, in case of an unallowed use of the motor vehicle KFZ the number of starts of the vehicle may be limited by suppressing the transfer of radio signals from the centre ZE to the motor vehicle KFZ. This suppression of the transfer of radio signals is for example possible by erasion of the individual identification number of the motor vehicle KFZ in the database of the centre ZE.

Fig. 4 shows a schematic diagram of the centre ZE of Fig. 1

The centre ZE incorporates a transmitting equipment SEN, a receiving equipment, a control unit UNIT having a comparator VER and a database DB.

The request signals of the security device SE are received via the receiving equipment EMP. The request signals are supplied to the comparator VER, which detects if the identification number in the respective request signal agrees with with a number stored in the database DB. Only in case of agreement the respective request signal is transferred. It is also possible to erase individual identification numbers in the database DB via the comparator VER, in order to present a transfer of the request signals and to suppress a transmission of the radio signals for individual motor vehicles.

The control unit UNIT comprises an exclusive-OR-gate XOR, an RSA encoding unit RSA, a read-only memory KEY1 for storing a secret key, and a generator GEN. The transferred request signals are supplied to the RSA-encoding unit RSA and to the generator GEN.

The exclusive-OR-gate XOR has two inputs and one output. The request signals are encoded in the RSA-encoding unit and are supplied five times to the first input of the exclusive-OR-gate XOR. Further, the request signals are supplied to the generator GEN. In the generator GEN five signals are generated which are sequentially supplied to the second input of the exclusive-OR-gate XOR. The first of the five signals comprises the count contained in the request signals. The second signal comprises the count increased by one unit. The third, fourth and fifth signals correspondingly contain the count increased by two, three and four units. The signals applied to the output of the exclusive-OR-gate XOR are supplied to the transmitting equipment SEN for transmission to the security device SE of the motor vehicle KFZ.

.....